up client (120) in such a way that a hacker cannot predict the field. A shared secret is added to the initial challenge and a pre-determined hashing algorithm is used so that the secret is not sent insecurely across a wire.

[0067] The ChallengeVal field is a sixteen-octet field that matches the ChallengeVal that appeared in a corresponding request packet. The Signature Length field is the length in octets of a signature. The signature field is the signature of the client computer (102) applied to the combination of ChallengeVal and ResponseVal. The client computer (102) takes the thirty-two octets formed by the ChallengeVal followed by the ResponseVal and produces a secure hash known by the server-side cryptographic function (130). The 128-bit message is then signed by the client-side cryptographic function (128) using the dial-up user's (120) private key. To verify this signature, the server-side cryptographic function (128) verifies the dial-up user's (120) signature using the dial-up user's (120) public key. The server-side cryptographic function (128) also produces a 128-bit hash using the ChallengeVal followed by the ResponseVal. The two results are then compared for equality.

[0068] In one or more embodiments, various different configurations of SmartDial may be implemented. Referring back to Figure 3, the dial-up client (120) may be isolated from the modem by a plurality of device drivers (140). For example, the Microsoft® telephony API (TAPI). The security management system insulates SmartDial from the device that contains the certificate (*i.e.*, smart card). SmartDial supports any device for storage of a certificate that is supported by the security management system.

[0069] In a particular embodiment, SmartDial may support only certificates issued by Entrust/Entelligence and only interfaces using the Entrust tool kit. SmartDial may support Steel Belted RADIUS (131) and use an SDK provided by Funk Software to interface with the LDAP-compliant directory service (113) and an

Entrust toolkit of high level APIs (130) on the server (112). The dial-up client (120) may support Microsoft® Windows NT and/or Windows 2000. In one embodiment, the certificate is managed by and is the responsibility of an external management system. Management of the smart card (106) may be external to SmartDial. Any security device (106) and card reader (104) that is supported by a Security Management System with a client-side cryptographic function (128) may be supported by SmartDial. Those skilled in the art will appreciate that the present invention is applicable to various other platforms and may be implemented in other ways.

[0070] Advantages of the present invention may include one or more of the following. SmartDial provides a secure way to handle network security with remote dial-up clients. SmartDial is a PKI-based authentication via dial-up connection while using security devices to digitally sign challenge. The private key is secure, as the key never leaves the card. SmartDial also supports two-way verification. Secure communication is also provided between the Remote Access Switch and the Server. SmartDial is also advantageous because the system uses industry standards to facilitate transition from existing methods. Because preexisting components are used, SmartDial can be integrated into existing systems to allow other trusted systems to perform authentication until all components are installed.

[0071] SmartDial is also advantageous because the system supports numerous protocols, including PPP, CHAP, EAP, RADIUS, and LDAP. Because SmartDial's Authentication Protocol is modeled after EAP, the implementation of SmartDial could easily tie into a Virtual Private Network (VPN) system to create end-to-end security when deemed necessary or cost effective. SmartDial uses PKI and can generate access tokens or encrypt data. Thus, the system can be extended to almost any VPN solution. Also, the software does not require any specialized

training or skills to use and user documentation is included in the form of an on-line context sensitive help system. Those skilled in the art will appreciate that the present invention may have further advantages.

[0072] While the invention has been described with respect to a limited number of embodiments, those skilled in the art, having benefit of this disclosure, will appreciate that other embodiments can be devised which do not depart from the scope of the invention as disclosed herein. Accordingly, the scope of the invention should be limited only by the attached claims.